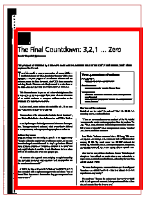
INFOSECURITY TODAY



N° and issue date : 40401 - 01/04/2004
Circulation : Unknown
Periodicity : Bimonthly
InfosecToday_40401_59_312.pdf
Web Site: http://www.elsevier.com/wps/find/journaldescription.cws_home/7
Page : 58
Size : 97 %

The Final Countdown: 3,2,1 ... Zero

Sarah Hilley *s.hilley@elsevier.com*

The prospect of infection by a network worm with no available patch is the stuff of bad dreams. Sarah Hilley explores the threat.

Top of the agenda at a recent congregation of security heads — the Global Council of CSOs, founded in November 2003 in San Francisco — was the prospect of an unknown infection with an unknown cause: the Zero day attack. And CSOs from companies including Oracle, Thomson, and Google zeroed in on the threat at the RSA conference held from 23-27 February in San Francisco.

This infection has not hit yet; it is still a theoretical nightmare. But it may not be so far away. As time from patch release to the arrival of an exploit continues to compress, evidence points to the possibility of a major Zero-day attack.

Such an attack occurs without the availability of a fix or even knowledge of the underlying vulnerability.

"It is the threat of the unknown that feeds the fear of this threat", says Gerhard Eschelbeck, vulnerabilities expert and CTO of Qualys.

Zero days belong to the third generation of electronic threats (see box, 'Three generations of malware'), which means that the payload is more poisonous, and targets specific geographies or industries.

A Zero-day worm

Zero day attacks with the ability to spread are the biggest worry. "Couple a Zero-day exploit with a replication engine and you can have that thing all around the world in a day," says Professor Richard Ford, at Florida Institute of Technology. Slammer is the proof that such rapid infection is possible. It took 10 minutes for it to infect 90% of all machines that it was ever going to get.

"It is easy to write a generic worm and plug an exploit in quickly. You don't need the exploit first," says Ford. "And it is possible to cut the time down dramatically."

A CERT manager at a leading UK Bank concurs that the exploit that is coupled with a replication engine is the real threat: "out of bound Zero days aren't a threat unless they get incorporated in a virus or worm."

Three generations of malware

First generation:

Needs user intervention – example MyDoom.

Second generation:

Leverages security holes – examples Slammer, Blaster.

Third generation:

Uses known and unknown vulnerabilities. Carries a more specific and powerful payload.

Aimed at particular geographies or industries. This is the generation of the Zero-day attack.

The fear of the unknown

Eschelbeck says he wouldn't be surprised if Zero day attacks were occurring now in a confined fashion.

"There are many attacks going on unnoticed on the Internet and some particular attacks are leveraging those Zero day exploits," he says. "They escape detection because the pattern is not known to IDS systems or firewalls". As a consequence, he warns, "attackers can easily conceal their activities".

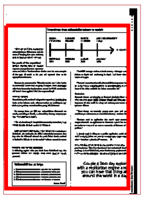
Last March, TruSecure announced that a US Army Web server was hacked into through a then unknown fault in Windows 2000 running IIS 5.0. The attack vector was WebDAV although the underlying vulnerability was in a core operating system component, according to Microsoft. The vendor hastily followed up with a fix.

Also late last year, a Linux distributor, Gentoo Technologies, is thought to have suffered an attack where a new vulnerability in rsync was used. Other Linux distributiors, affected by the same flaw, rapidly released patches.

The senior banking source mentioned above says: "the really good Zero-days are probably kept hold of and used against one or two organisations very quietly."

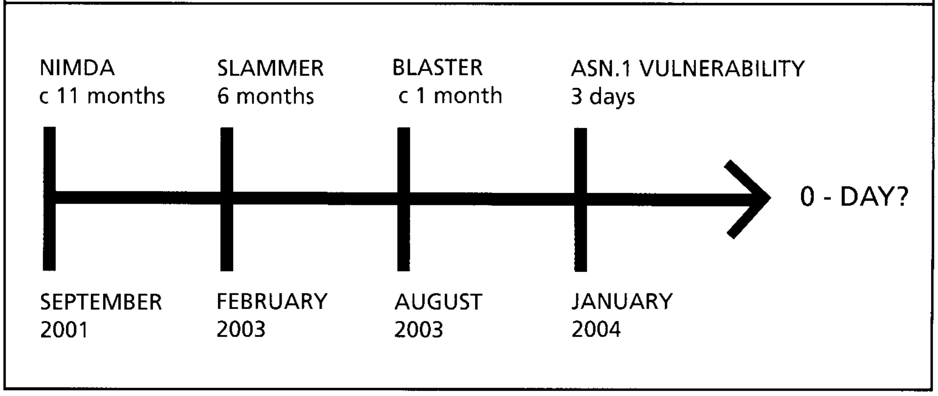
He continues: "Because the underground community is riddled with federal agents and commercial alert providers stuff that is Zero day and remains Zero day is quite rare."

INFOSECURITY TODAY



N° and issue date : 40401 - 01/04/2004
Circulation : Unknown
Periodicity : Bimonthly
InfosecToday_40401_59_312.pdf
Web Site: http://www.elsevier.com/wps/find/journaldescription.cws_home/7
Page : 59
Size : 94 %

"There are black hats searching for vulnerabilities in Web servers with the intent of keeping them quiet and using them for their own gain," he warns.



Countdown from vulnerability release to exploit

The perils of the unpatched

Richard Starnes, head of incident response, managed security operations centre at Cable & Wireless admits that his team has seen examples of this type of attack in the past and reported them to the appropriate authorities.

However, he points out that "Zero day attacks aren't what bother me excessively because they are going to happen. What bothers me is the fact that patches that have been around for 18-24 months that still haven't been applied. I find that very troubling".

Held to ransom

Nevertheless, with armies of independent researchers breaking their backs to dig holes in code, software vendors are walking on egg-shells trying to keep researchers from going full disclosure.

On average there are 200 new vulnerabilities discovered per month, according to Sintelli, a vulnerability alerting company (see box, 'Vulnerabilities at large').

"The whole industry is being held to ransom by researchers," says Marcus Ranum, research scientist at TruSecure.

Eighty per cent of exploits arise within 80 days now, according to Eschelbeck. An exploit for the ASN.1 vulnerability came just three days after the Microsoft released the patch. When Nimda surfaced in September 2001 the fix for the exploit had been around for a year.

Looking out for the unknown

In defending against what you don't know, Eschelbeck says that perimeter defence isn't enough. Every device must be equally protected.

Vulnerabilities at large

1. 220 vulnerabilities recorded between 1-jan-2004 and 31-jan-2004
2. 225 vulnerabilities recorded between 1-feb-2004 and 29-feb-2004
3. 198 vulnerabilities recorded between 1-dec-2003 and 31-dec-2003
4. 198 vulnerabilities recorded between 1-nov-2003 and 30-nov-2003
5. 222 vulnerabilities recorded between 1-oct-2003 and 31-oct-2003

Source: Sintelli

The CERT manager at the UK bank concurs: "what you need is defence in depth and monitoring in depth. And know what is important to you.

"You need to monitor firewalls. Network IDS is no panacea but it is a useful tool, as is host-based IDS. As for specific tools, Tripwire is one of the oldest available but it does an excellent job".

Evolution

Electronic threats are changing as financial criminals elbow into what was once script kiddie territory. Mimail and Sobig are the beginnings of what could be a long and enduring virus writer and spammer alliance.

"These things are certainly getting more press and more mindshare, so it does seem an inevitable evolution," confirms Ford.

"Slammer used an application that wasn't super common, imagine that with an application we don't have a patch for and is extremely common, and you start to get an idea of the scope of the problem."

A ghostly exploit riding on a prolific application could circle world networks before the security industry could know what is what — let alone update its AV scanners. ■

Note: At Infosec (27-29 April), Qualys is staging an interactive panel session on "Zero Day Attacks and how to deal with them", involving Gerhard Eschelbeck, senior level security professionals and PricewaterhouseCoopers. You can visit Qualys at stand 360.

Couple a Zero day exploit with a replication engine and you can have that thing all around the world in a day